Benutzerhandbuch - Deutsch

FUJITSU Software ServerView Windows Server Integration Pack V8.0 for MS SCOM 2012

Ausgabe Juni 2015

© Copyright Fujitsu Technology Solutions GmbH 2015

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Alle Rechte vorbehalten, insbesondere (auch auszugsweise) die der Übersetzung, des Nachdrucks, der Wiedergabe durch Kopieren oder ähnliche Verfahren.

Zuwiderhandlungen verpflichten zu Schadenersatz.

Alle Rechte vorbehalten, insbesondere für den Fall der Patenterteilung oder GM-Eintragung.

Lieferung nach Verfügbarkeit. Technische Änderungen vorbehalten.

Inhalt

1. Einleitung 1

1.1 Zielgruppen und Zielsetzung 1

1.2 Änderungen gegenüber der vorigen Ausgabe 2

1.3 ServerView Suite Link-Sammlung 3

1.4 Dokumentation zur ServerView Suite 4

1.5 Darstellungsmittel 5

2. Integrationsvoraussetzungen 7

2.1 Trap-Gewichtungen für ServerView Agents einstellen 8

2.2 ServerView Agents aktualisieren 9

3. Installation und Deinstallation 11

3.1 ServerView Integration Pack installieren 11

3.1.1 Installierte Dateien 11

3.1.2 Nur SCOM-Konsole 12

3.1.3 Management Packs importieren 12

3.2 Update auf eine neue Version 12

3.3 ServerView Integration Pack deinstallieren 13

3.4 ServerView Library Management Pack aktualisieren 13

4. Eigenschaften des ServerView Windows Server Integration Packs 15

4.1 Management Packs 15

4.2 PRIMERGY Server Computer-Gruppen 16

4.3 Ermittlung und Überwachung der PRIMERGY Server 16

4.3.1 Angezeigte Eigenschaften erkannter PRIMERGY Server 17

4.3.2 Gesundheitszustand eines PRIMERGY Servers 17

4.3.3 Virtuelle Maschine wird als PRIMERGY Server erkannt 18

4.4 Server-Komponenten erkennen und überwachen 18

4.4.1 Hardware-Subsysteme (Komponenten) erkennen 19

4.4.1.1 PRIMERGY Overall State - Gesamtstatus eines PRIMERGY Servers 19

4.4.1.2 Processors - Prozessoren 19

4.4.1.3 Memory - Speichermodule 20

4.4.1.4 Storage - Speichergeräte ... 20
4.4.1.5 Networks (Ethernet) - Netzwerke (Ethernet) ... 20
4.4.1.6 Management Controller - Management-Controller ... 21
4.4.1.7 Fans (Cooling) - Lüfter (Kühlung) ... 21
4.4.1.8 Temperatures - Temperaturen ... 21
4.4.1.9 Power Supplies - Stromversorgungen ... 22
4.4.1.10 Power Consumption - Stromverbrauch ... 22
4.4.1.11 Voltages - Spannungssensoren ... 22
4.4.1.12 RAID Subsystem - RAID-Subsystem ... 23
4.4.1.13 RAID Logical Drive - Logisches RAID-Laufwerk ... 23
4.4.1.14 RAID Logical Drives - Logische RAID-Laufwerke ... 23
4.4.1.15 RAID Physical Disks - Physische RAID-Laufwerke ... 24
4.4.2 Status der Hardware-Subsysteme aktualisieren ... 24
4.4.3 Ermittlung der benötigten Dienste ... 24
4.4.3.1 ServerView Agents ... 25
4.4.3.2 Windows Management Instrumentation (WMI) ... 25
4.4.3.3 ServerView RAID ... 25
4.4.4 Überwachung der Hardware-Komponenten ... 26
4.4.5 Überwachung der benötigten Dienste ... 26
4.4.5.1 SCCI Management Software (ServerView Agents) ... 26
4.4.5.2 Windows Management Instrumentation (WMI) ... 26
4.4.5.3 ServerView RAID Manager ... 27
4.5 Ansichten ... 28
4.5.1 Vom MP *Fujitsu Systems Core Library* definierte Ansichten ... 28
4.5.2 Vom MP *Fujitsu PRIMERGY Windows Servers* definierte Ansichten ... 29
4.5.3 Ansicht "Active Alerts" ... 29
4.5.4 Ansichten "Health State Collection" ... 30
4.5.5 Ansichten "Diagram" ... 30
4.5.6 Ansicht Server State ... 31
4.6 Integritäts-Explorer ... 31
4.7 Aufgaben für Fujitsu PRIMERGY Windows Server ... 32
4.7.1 Computer Management ... 33
4.7.2 Remote Desktop ... 33
4.7.3 Remote Desktop Console ... 33
4.7.4 Delete PRIMERGY Server Component Inventory ... 33
4.7.5 ServerView Raid Manager ... 34
4.7.6 ServerView Remote Management iRMC ... 34
4.7.7 ServerView System Monitor ... 34
4.8 Ereignisse und Alarme ... 34
4.8.1 Aktivierung und Deaktivierung von Alarmen ... 35

4.9 Wissensdatenbank ... 36

5. Anhang ... 37

5.1 Unterstützte PRIMERGY Server ... 37

5.2 Einträge in der Ereignisanzeige des Operations Managers ... 37

5.3 Test-Einträge in der Windows Ereignisanzeige erzeugen ... 38

5.4 Log-Dateien anlegen ... 38

5.4.1 Aktualität der Log-Dateien ... 39

5.5 Aktualisierung älterer Versionen des Windows Server Integration Packs ... 39

5.5.1 Migration von Versionen vor V8.0 ... 40

5.6 Fehlersuche ... 41

5.6.1 ServerView System Monitor zur Untersuchung eines PRIMERGY Servers verwenden ... 41

5.6.2 Kein Ereignis-Logging auf den Controller-Laufwerken ... 41

5.6.3 Internet Explorer hat kein Java-Plugin ... 41

5.6.4 Windows Installer-Logging aktivieren/deaktivieren (Debug) ... 42

5.7 Tipps und bekannte Probleme ... 42

6. Anhang B ... 43

6.1 V8.0 Klassennamen und vorherige Namen ... 43

1. Einleitung

Die PRIMERGY ServerView Suite von Fujitsu Technology Solutions bietet zahlreiche ServerView-Integrationsmodule, mit denen sich PRIMERGY Server auf einfache Art und Weise in andere Enterprise Management-Systeme integrieren lassen.

Dieses Handbuch beschreibt das ServerView Windows Server Integration Pack V8.0, mit dem der Fujitsu PRIMERGY ServerView Operations Manager in den System Center 2012 Operations Manager (SCOM 2012) integriert werden kann. Es werden alle SCOM 2012-Editionen bis zu SCOM 2012 R2 unterstützt.

Mit diesem Integration Pack lassen sich die PRIMERGY Windows Server von Fujitsu Technology Solutions über SCOM überwachen. Die Überwachung eines Fujitsu PRIMERGY Windows Servers wird insbesondere durch Monitore von Hardware- und Software-Komponenten realisiert und durch Symbole angezeigt.

Wenn bei der Hardware-Überwachung eines PRIMERGY Windows-Servers Fehler auftreten, so werden diese vom ServerView Agent als Ereigniseinträge in die Windows-Ereignisanzeige (Windows EventLog) des verwalteten Servers geschrieben. Diese Ereignisse werden vom SCOM-Agenten, der sich auf den überwachten Systemen befindet, zur SCOM-Management-Station geschickt und hier in der SCOM-Konsole entsprechend den Einstellungen durch das Management Pack ausgewertet und angezeigt.

Desweiteren können Regeln angewendet werden, die beim Auftreten eines Fehlers eine entsprechende Aktion auslösen, z. B. das Senden einer Mail mit Fehlerbeschreibung an den Hardware-Support.

Für eine detaillierte Analyse kann der ServerView System Monitor gestartet werden.

Das aktuelle ServerView Windows Server Integration Pack for SCOM 2012 erhalten Sie mit der neuesten PRIMERGY ServerView Suite DVD von Fujitsu Technology Solutions oder als Download von der Webseite:

http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/

1.1 Zielgruppen und Zielsetzung

Das vorliegende Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Kenntnisse von Hardware und Software verfügen. Desgleichen werden solide Grundkenntnisse des Microsoft System Center Operations Manager 2012 vorausgesetzt.

1.2 Änderungen gegenüber der vorigen Ausgabe

Das ServerView Windows Server Integration Pack V8.0 enthält die folgenden Änderungen und neuen Funktionen:

- Fujitsu Management Packs wurden generell umstrukturiert, um die Integration aller Fujitsu Management Packs auf vereinfachte Weise zu ermöglichen.
  Für das ServerView Windows Server Integration Pack bedeutet das folgende Änderungen:
  - Das vormals monolithische Management Pack wurde in eine Management Pack-Suite mit einzelnen MPs aufgeteilt.
  - Der Standardinstallationsordner wurde von *"%ProgramFiles(x86)%\Fujitsu\ServerView Suite\SCOM Integration"* zu *"%ProgramFiles%\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-Win"* geändert.
  - Die Dateistruktur im Installationsordner wurde geändert. Siehe Kapitel 3.1.1 Installierte Dateien
  - Die Klassen und Objektnamen innerhalb des ServerView Windows Server Integration Packs mussten geändert werden. Alle kundenseitigen Packs für die Außerkraftsetzung oder Skripte, die sich auf MP-Objekte richten, müssen wahrscheinlich angepasst werden. Siehe Kapitel 5.5.1 Migration von Versionen vor V8.0 für weitere Details.
- Die Komponentenverfolgung wurde dem ServerView Windows Server Integration Pack hinzugefügt. Siehe Kapitel 4.7.4 Delete PRIMERGY Server Component Inventory für weitere Details.
- Eine Aufgabe für das Zurücksetzen von Komponentenverfolgungsdaten wurde hinzugefügt. Siehe Kapitel 4.7.4 Delete PRIMERGY Server Component Inventory für weitere Details.
- Die Variable "DebugString" für Ermittlungsdatenquellen wurde entfernt. Das Debuggen wird jetzt ausschließlich über die Datei "SVISCOMLog.ini" gesteuert. Siehe Kapitel 5.4 Log-Dateien anlegen für weitere Details.
- Eine neue Aufgabe für den Aufruf des Web-basierten ServerView System Monitors wurde hinzugefügt.
- Aufgaben für den Aufruf vom ServerView Operations Manager wurden entfernt.

1.3 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt den Kunden über die Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Service Desk
- Handbücher
- Produktinformationen
- Sicherheitsinformationen
- Software Downloads
- Schulungen

Die Downloads umfassen u. a.:

- aktuelle Software-Stände zur ServerView Suite und ergänzende Readme-Dateien.
- Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView Agents und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
- die aktuelle Version aller Dokumentationen zur ServerView Suite

Alle Downloads vom Fujitsu Technology Solutions-Web-Server sind kostenlos.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Service Desk
- Handbücher
- Produktinformationen
- Ersatzteilkatalog

Zugriff auf die ServerView Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. über den ServerView Operations Manager
   - Wählen Sie auf der Startseite bzw. in der Menüzeile *Help – Links* aus. Anschließend wird die Startseite der Link-Sammlung angezeigt.
2. über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions.

   Die Startseite der Online-Dokumentation finden Sie unter *http://manuals.ts.fujitsu.com*
   - Wählen Sie links in der Auswahlliste *x86 Servers*.
   - Klicken Sie auf den Menüpunkt *PRIMERGY ServerView Links*. Anschließend wird die Startseite der Link-Sammlung angezeigt.
3. über die ServerView Suite DVD.
   - Markieren Sie im Startfenster der ServerView Suite DVD die Option *ServerView Software Produktauswahl*.
   - Klicken Sie auf *Start*, um die Seite mit den Software-Produkten der ServerView Suite aufzurufen.
   - Klicken Sie in der Menüzeile auf *Links*, um die Startseite der ServerView Link-Sammlung aufzurufen.

1.4 Dokumentation zur ServerView Suite

Die Dokumentation ist über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation zur ServerView Suite finden Sie unter *http://manuals.ts.fujitsu.com* und dem Link x86 Servers.

Einen Überblick über die Dokumentation, die Sie unter ServerView Suite finden, sowie die Ablagestruktur erhalten Sie auf der ServerView Suite Sitemap (*ServerView Suite - Site Overview*).

1.5 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

	Warnung Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Information Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben.
▸	Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt.
Kursive Schrift	Im Fließtext werden Kommandos, Menüpunkte, Namen von Schaltflächen, Optionen, Dateinamen und Pfadnamen kursiv dargestellt.
<variable>	Angaben zwischen spitzen Klammern kennzeichnen Variablen, die durch Werte ersetzt werden.

Bildschirmausgaben

Beachten Sie bitte, dass die Bildschirmausgaben nicht in allen Details mit der Ausgabe auf Ihrem System übereinstimmen müssen. Ebenso können bezüglich der verfügbaren Menüpunkte systembedingte Unterschiede auftreten.

2. Integrationsvoraussetzungen

Die im Folgenden aufgeführten Voraussetzungen müssen für die Integration erfüllt sein.

Management-Station

- Microsoft System Center 2012 Operations Manager
- Windows Server 2008 R2 / 2012 / 2012 R2.
  siehe Voraussetzungen zu der jeweiligen SCOM Version
- SQL Server 2008 / 2012 / 2014.
  siehe Voraussetzungen zu der jeweiligen SCOM Version

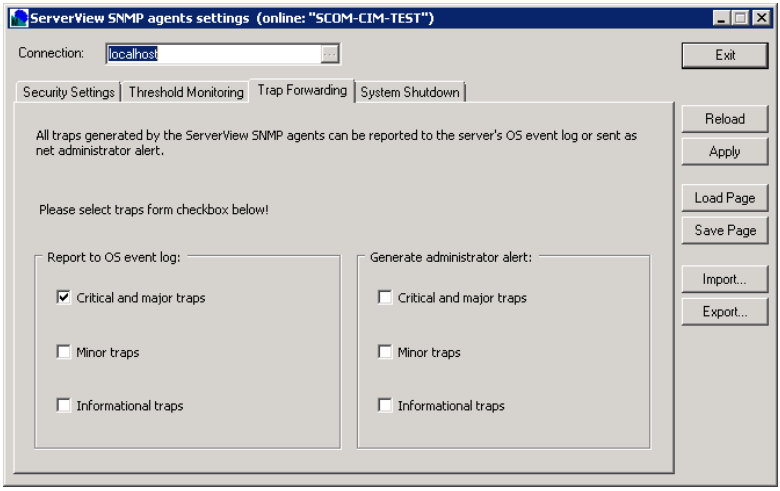
Verwaltete PRIMERGY Server

- Windows Server 2008 [R2] oder Windows Server 2012 [R2]
- Windows Management Instrumentation (WMI)
- ServerView Agents ab V6.00.04
  Für Windows Server 2012 und höher verwenden Sie Agenten ab V6.12.xx (V6.20.xx ausgeschlossen)
- ServerView RAID für RAID-Überwachung
- Management Controller iRMC (integrated Remote Management Controller) (für die Überwachung des Stromverbrauchs)
- Installierter SCOM-Agent

2.1 Trap-Gewichtungen für ServerView Agents einstellen

Damit ServerView-Ereignisse in SCOM angezeigt werden können, müssen sie in die Windows Ereignisanzeige geschrieben werden. Für ServerView Agents müssen dazu die gewünschten Trap-Gewichtungen (Trap Severities) aktiviert werden.

Öffnen Sie über das Startmenü (*Start > [Alle] Programme > Fujitsu > ServerView Suite > Agenten > Agenten-Konfiguration*) das folgende Dialogfeld, und aktivieren Sie auf der Registerkarte *Trap Forwarding* unter *Report to system event log* die erforderlichen Trap-Gewichtungen.



2.2 ServerView Agents aktualisieren

Wenn Sie ServerView Agents aktualisieren wollen, setzen Sie den entsprechenden PRIMERGY Server während dieses Vorgangs in den Wartungsmodus.

Wenn die Zielserver, auf denen die ServerView Agents aktualisiert werden sollen, nicht im Wartungsmodus sind, werden die ServerView Agents möglicherweise nicht vollständig installiert.
Dies kann sich auf die Überwachungsfunktionen der ServerView Agents und des ServerView Windows Server Integration Packs auswirken.

3. Installation und Deinstallation

3.1 ServerView Integration Pack installieren

Das Installationsprogramm *SVISCOM-Win.exe* befindet sich auf der ServerView Suite DVD unter

<DVDroot>\SVSSoftware\Software\Integration_Solutions\SCOM

Alternativ können Sie es auch unter folgendem Link von der Website herunterladen:

http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/

Das Installationsprogramm führt zuerst einige Basisprüfungen durch und startet dann den Installation Wizard. Folgen Sie den Anweisungen, die Sie während des Installationsvorgangs erhalten.

3.1.1 Installierte Dateien

Der Standard-Installationspfad auf der Management-Station lautet:

- *%ProgramFiles%\Fujitsu\ServerView Suite\SCOM Integration*

Folgende Dateien werden in die Installationsverzeichnisse kopiert:

Ordner	**Dateien**
SVSICOM-Win Unterverzeichnis	• *EULA_en.pdf* • *EULA_jp.pdf* • *PRIMERGYServerEventsSCOM_en.pdf* • *sv-intpack-scom-win-en.pdf* • *windows_manual_elx.pdf*
Management Packs Unterverzeichnis	• *Fujitsu.ServerView.Library.mp* • *Fujitsu.Servers.PRIMERGY.WindowsSeed.mp* • *Fujitsu.Servers.PRIMERGY.Windows.mp* • *Fujitsu.Servers.PRIMERGY.Windows.SC2MIB.Alerts.mp* (optional) • *Fujitsu.Servers.PRIMERGY.Windows.RAIDMIB.Alerts.mp* (optional)

Rufen Sie nach der Installation mit folgendem Befehl die SCOM-Konsole auf: *Microsoft.EnterpriseManagement.Monitoring.Console.exe /clearcache*.

3.1.2 Nur SCOM-Konsole

Um ServerView System Monitor und iRMC Remote Management über einen Server aufzurufen, der nur über die SCOM-Konsole verfügt, installieren Sie das ServerView Windows Server Integration Pack auf allen Servern mit SCOM-Konsolen, über die beide Websites aufgerufen werden.

Schließen Sie die Konsole einmal nach der Installation, um sicherzustellen, dass die Konsole alle neuen Umgebungsvariablen liest.

3.1.3 Management Packs importieren

Vom ServerView Windows Server Integration Pack installierte Management Packs befinden sich im Installationsordner im Ordner "Management Packs". Dieser Ordner enthält alle Management Packs aus ServerView Integration Packs für System Center Operations Manager und nicht nur aus dem ServerView Windows Server Integration Pack.

Die Management Packs werden in üblicher Weise über die SCOM-Konsole importiert.

Um die Management Packs zu importieren, sind SCOM-Administratorrechte nötig.

Alle Management Packs des ServerView Windows Server Integration Packs müssen importiert werden. Siehe Kapitel 3.1.1 Installierte Dateien für weitere Details. Sie können alle gleichzeitig installiert werden.

3.2 Update auf eine neue Version

Die Update-Installation wird vom ServerView Windows Server Integration Pack nicht unterstützt. Stattdessen wird zunächst die alte Version vollständig deinstalliert und dann die neue Version installiert.

Befolgen Sie die Anweisungen in Kapitel 3.3 ServerView Integration Pack deinstallieren, um das alte ServerView Windows Server Integration Pack zu deinstallieren.

Befolgen Sie die Anweisungen in Kapitel 3.1 ServerView Integration Pack installieren, um das neue ServerView Windows Server Integration Pack zu installieren.

3.3 ServerView Integration Pack deinstallieren

Das ServerView Windows Server Integration Pack wird über die folgenden Schritte deinstalliert:

- Entfernen Sie alle Management Packs für die Außerkraftsetzung (sofern vorhanden) von SCOM.
  Wenn bestehende Außerkraftsetzungswerte beibehalten werden sollen (z. B. zur Wiederverwendung in einer neuen Version), dann sollten die Management Packs für die Außerkraftsetzung exportiert und gespeichert werden.
- Entfernen Sie die PRIMERGY Windows Server Management Packs von SCOM.

  Wenn andere ServerView Integration Packs für System Center Operations Manager installiert wurden, sollte das ServerView Library Management Pack nicht deinstalliert werden.

- Deinstallieren Sie das ServerView Windows Server Integration Pack vom SCOM-Server.

Für das Entfernen der Management Packs benötigen Sie SCOM-Administratorrechte. Das ServerView Windows Server Integration Pack sollte von allen SCOM-Remote-Konsolen entfernt werden.

3.4 ServerView Library Management Pack aktualisieren

Das ServerView Library Management Pack wird von allen Fujitsu ServerView Integration Packs für System Center Operations Manager verwendet und referenziert.

Wenn ein ServerView Integration Pack eine neuere Version des ServerView Library Management Packs installiert, müssen alle Fujitsu Management Packs, einschließlich deren Management Packs für die Außerkraftsetzung, deinstalliert und alle Fujitsu Management Packs aus dem Ordner "Management Packs" zusammen mit dem aktualisierten ServerView Library Management Pack neu installiert werden.

4. Eigenschaften des ServerView Windows Server Integration Packs

4.1 Management Packs

Das Management Pack *Fujitsu ServerView Core Library* enthält die grundlegenden Definitionen für die konsolidierte Verwaltung von Fujitsu-Systemen in SCOM. Dieses Management Pack wird mit allen Fujitsu SCOM Integration Packs verteilt. Es kann nicht verändert oder exportiert werden.
Der Dateiname dieses Pakets lautet *Fujitsu.ServerView.Library.mp*.

Das Management Pack *Fujitsu PRIMERGY Windows Servers Seed* enthält die ursprüngliche Fujitsu PRIMERGY Windows Server Discovery. Es kann nicht verändert oder exportiert werden.
Der Dateiname dieses Pakets lautet *Fujitsu.Servers.PRIMERGY.WindowsSeed.mp*.

Das Management Pack *Fujitsu PRIMERGY Windows Servers* enthält die Definitionen für die Ermittlung und Überwachung von Fujitsu PRIMERGY Servern, die auf Windows-Betriebssystemen ausgeführt werden. Es kann nicht verändert oder exportiert werden.
Der Dateiname dieses Pakets lautet *Fujitsu.Servers.PRIMERGY.Windows.mp*.

Das SC2.MIB Alerts Management Pack *Fujitsu PRIMERGY Windows Servers* enthält Regeln für das Erfassen von Alarmen bei Fehlern und Warnungen aus dem ServerView-Hardware-MIB "SC2.mib".
Dieses Management Pack ist nicht erforderlich, um eine vollständige Überwachung von PRIMERGY Windows Servern sicherzustellen, sondern wird für Kunden bereitgestellt, die Statusänderungen für Hardware nicht nur anzeigen, sondern alle Hardwareereignisse als einzelne Alarme erhalten möchten.
Der Dateiname dieses Pakets lautet *Fujitsu.Servers.PRIMERGY.Windows.SC2MIB.Alerts.mp*.

Das RAID.MIB Alerts Management Pack *Fujitsu PRIMERGY Windows Servers* enthält Regeln für das Erfassen von Alarmen bei Fehlern und Warnungen aus dem ServerView-RAID-MIB "RAID.mib".
Dieses Management Pack ist nicht erforderlich, um eine vollständige Überwachung der RAID-Umgebung von PRIMERGY Windows Servern sicherzustellen, sondern wird für Kunden bereitgestellt, die Statusänderungen für die RAID-Umgebung des Servers nicht nur anzeigen, sondern alle RAID-Ereignisse als einzelne Alarme erhalten möchten.
Der Dateiname dieses Pakets lautet *Fujitsu.Servers.PRIMERGY.Windows.RAIDMIB.Alerts.mp*.

4.2 PRIMERGY Server Computer-Gruppen

Die PRIMERGY Server sind in Gruppen eingeteilt:

- BX-Modelle (z.B. BX920)
- CX-Modelle (z.B. CX122)
- MX-Modelle (z.B. MX130)
- RX-Modelle (z.B. RX100, RX300)
- SX -Modelle (z.B. SX150, SX350)
- TX-Modelle (z.B. TX150, TX300)
- PRIMERGY Modelle, die in keine der obigen Gruppen passen

Econel-Modelle werden in die Gruppe der TX-Modelle (Econel Floorstand) oder RX-Modelle (Econel 230R) einsortiert.

Eine Beschreibung zur Darstellung der Server und der PRIMERGY Server Computer-Gruppen finden Sie im Abschnitt "Ansichten" auf Seite 28.

4.3 Ermittlung und Überwachung der PRIMERGY Server

Die Ermittlung und die Überwachung der PRIMERGY Server und ihrer Komponenten funktioniert nur, wenn sie in die SCOM-Verwaltung aufgenommen worden sind (installierter SCOM-Agent auf den zu überwachenden Servern).

Die ursprüngliche Ermittlung (Seed) erfolgt, indem die Registry des Zielservers in den Abschnitten "SystemInformation" und "Bios" auf Hersteller und Systemtyp überprüft wird.

Die Server werden dann über Skripte und auf der Grundlage der von WMI- und ServerView CIM-Providern bereitgestellten Daten erkannt und überwacht.

Es werden nur Server mit folgenden Hersteller- und Modellangaben erkannt:

— Hersteller: Fujitsu ... oder FUJITSU ... oder FSC

— Modell: PRIMERGY ...

Die Modellerkennung erfolgt über die Chassis-Bezeichnung.

4.3.1 Angezeigte Eigenschaften erkannter PRIMERGY Server

Folgenden Eigenschaften (Properties) eines verwalteten Servers werden angezeigt:

- *Display Name*: Rechnername des Servers
- *Network Name:* vollqualifizierter DNS-Name des Servers
- *Model*: Kompletter Modellname des Servers
- *Serial Number*: Seriennummer des Servers
- *Operating System:* detaillierte Version des Betriebssystems
- *Manufacturer*: Hersteller des Systems
- *Chassis Model*: Chassis-Bezeichnung
- *Cabinets:* IDs von Haupt- und Erweiterungsschränken
- *System Firmware*: Version der System-Firmware
- *Physical Memory*: Verfügbarer Arbeitsspeicher
- *Total Logical Disk Space*: Summe der als logische Platten konfigurierten Partitionen
- *Monitoring Agents*: Name und Version der ServerView Agents
- *BMC Address*: IPv4-Adresse des iRMC falls vorhanden)
- *BMC DNS name:* vollqualifizierter DNS-Name des iRMC (falls vorhanden)

Die ermittelten Eigenschaften eines Servers werden in der *Detailansicht* unterhalb einer Status- oder einer Diagramm-Ansicht angezeigt.

4.3.2 Gesundheitszustand eines PRIMERGY Servers

Der Gesundheitszustand eines PRIMERGY Servers wird durch den Zustand seiner Hardware- und Software-Komponenten bestimmt. Die Komponente mit dem schwerwiegendsten Fehler bestimmt den finalen Gesundheitszustand eines PRIMERGY Servers. Das heißt, Komponentenredundanz wird nicht unterstützt.

Dieser Status wird auch in die Modell-Gruppe und in die PRIMERGY Server-Gruppe hochgereicht (Rollup-Monitor).

4.3.3 Virtuelle Maschine wird als PRIMERGY Server erkannt

Virtuelle Maschinen sind für die Überwachung mit dem Fujitsu Management Pack nicht vorgesehen.

Wenn eine virtuelle Maschine als PRIMERGY Server erkannt und in die Monitoring-Aktivitäten aufgenommen wird (z. B. weil ein physischer PRIMERGY Server in eine virtuelle Maschine konvertiert wurde), dann weil die Werte für die Erkennung des PRIMERGY Servers noch in der Registry gespeichert sind.

Um die virtuelle Maschine aus dem SCOM-Monitoring zu entfernen, müssen Sie die virtuelle Maschine in den Wartungsmodus setzen und den folgenden Eintrag in der Registry sowie seinen gesamten Inhalt löschen:

HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-Win\PYServerData
oder
HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\ServerView Suite\SCOM Integration\PYServerData

4.4 Server-Komponenten erkennen und überwachen

Die Erkennung und Überwachung der Server-Komponenten erfolgt anhand von Skripten auf Basis der Daten, die über die CIM-Provider (WMI) der ServerView Agents abgerufen werden, über den ServerView-RAID-Agenten und gelegentlich über andere ServerView Agent APIs.

In der Diagramm-Ansicht werden nur Komponenten angezeigt, die vorhanden sind. Wenn z. B. kein Lüfter ermittelt werden kann (z. B. bei einem Blade Server, bei dem Lüfter über das Gehäuse verwaltet werden), wird die Komponente nicht angezeigt. Subsysteme, die zum Ermittlungszeitpunkt keine Komponenten mit einem verwendbaren Status enthalten, werden ebenfalls nicht angezeigt. Alle Komponenten werden im Integritäts-Explorer angezeigt, aber nur vorhandene Komponenten werden überwacht.

Gleichartige Instanzen einer Komponente werden zu einer Gruppe zusammengefasst und gemeinsam überwacht (Beispiel: die einzelnen CPUs eines Servers gehören zur Gruppe der Prozessoren). Im Fehlerfall wird die fehlerhafte Instanz im Integritäts-Explorer angezeigt. Die Instanz mit dem schwerwiegendsten Fehler bestimmt den Gesamtstatus der Gruppe.

Per Voreinstellung erzeugen alle Ereignisse mit der Gewichtung *Kritisch* einen Alarm und alle Ereignisse mit der Gewichtung *Warnung* erzeugen keinen Alarm. Diese Standardeinstellung kann überschrieben werden.

4.4.1 Hardware-Subsysteme (Komponenten) erkennen

Die im Folgenden aufgeführten Hardware-Subsysteme eines PRIMERGY Servers können ermittelt und überwacht werden.

4.4.1.1 PRIMERGY Overall State - Gesamtstatus eines PRIMERGY Servers

Durch diese Komponente wird der Gesamtstatus eines PRIMERGY Servers dargestellt und überwacht. Hier werden auch Komponenten überwacht, die durch die im Folgenden beschriebenen speziellen Hardware-Komponenten nicht erfasst werden. Verwenden Sie die Aufgabe "ServerView System Monitor", um detaillierte Informationen anzuzeigen.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	PRIMERGY Overall State *<Name des Servers>* *<Überwachte Komponenten>* Keine *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

Kommunikationsüberwachung im "PRIMERGY Overall State"

Der "PRIMERGY Overall State" beinhaltet auch eine Kommunikationsüberwachung, die die Kommunikation zwischen den von SCOM ausgeführten Skripten und dem Dienst der ServerView Agents überwacht.

Probleme hier zeigen an, dass die Hardware-Überwachung beeinträchtigt ist. Starten Sie den Dienst "ServerView Server Control" neu und verwenden Sie deie Aufgabe "ServerView System Monitor", um detaillierte Informationen anzuzeigen.

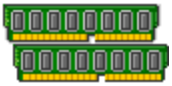
4.4.1.2 Processors - Prozessoren

Es werden die physisch vorhandenen Prozessoren ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Processors *<Name des Servers>* *<Namen der physischen CPUs>* *<CPU-Typ/Anzahl der Kerne>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.3 Memory - Speichermodule

Es werden die angeschlossenen Speichermodule ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	*Display Name:* *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Memory *<Name des Servers>* <Gesamtspeicher> <Speichertyp>: <Anzahl der Speicher des Typs> *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.4 Storage - Speichergeräte

Es werden die verfügbaren Speichergeräte ermittelt, deren Daten angezeigt und der Integritätsstatus überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Storage *<Name des Servers>* *<Speichergerätes>* *<Kapazität der Speichergeräte>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC*

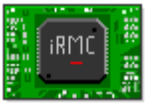
4.4.1.5 Networks (Ethernet) - Netzwerke (Ethernet)

Es werden die verfügbaren Netzwerkkarten ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Networks (Ethernet) *<Name des Servers>* *<Namen der Netzwerk-Adapter/Schnittstellen>* *<MAC-Adressen>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.6 Management Controller - Management-Controller

Der iRMC (integrated Remote Management Controller) wird ermittelt, seine Daten werden angezeigt und sein Gesundheitszustand wird überwacht.

Symbol	Information	
	*Display Name:* *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Management Controller *<Name des Servers>* *<Typ>* Firmware Version: *<Version>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.7 Fans (Cooling) - Lüfter (Kühlung)

Es werden die angeschlossenen Lüftermodule des PRIMERGY Servers und eventuelle Erweiterungsmodule ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Fans (Cooling) *<Name des Servers>* *<Typ>* Firmware Version: *<Version>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.8 Temperatures - Temperaturen

Es werden die physisch vorhandenen Temperatursensoren ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Temperatures *<Name des Servers>* *<Typ>* Firmware Version: *<Version>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.9 Power Supplies - Stromversorgungen

Es werden die physisch vorhandenen Stromversorgungsmodule ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Power Supplies *<Name des Servers>* <Stromversorgungen> *Keine* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.10 Power Consumption - Stromverbrauch

Der Stromverbrauch wird überwacht, wenn der iRMC die Überwachung des Stromverbrauchs unterstützt und wenn der *Modus der Energieverbrauchssteuerung* des iRMC auf *Power Limit* gesetzt ist. Wenn der Modus der Energieverbrauchssteuerung auf irgendeinen anderen Modus gesetzt ist, zeigt die Überwachung des Stromverbrauchs immer "OK" an.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Power Consumption *<Name des Servers>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>* Gesamtverbrauch Keine

4.4.1.11 Voltages - Spannungssensoren

Es werden die physisch vorhandenen Spannungssensoren ermittelt, deren Daten angezeigt und der Gesundheitszustand überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	Voltages *<Name des Servers>* *Number of Voltages: <Nummer>* *Keine* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.12 RAID Subsystem - RAID-Subsystem

Wenn ServerView RAID installiert ist, werden SV RAID und alle RAID-Adapter ermittelt, ihre Daten werden angezeigt und ihr Integritätsstatus wird überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	RAID Subsystem *<Name des Servers>* *ServerView RAID, <RAID-Adapter>* <Version/Typ> *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.13 RAID Logical Drive - Logisches RAID-Laufwerk

Der Status der logischen RAID-Laufwerke von ServerView RAID wird über die ServerView Agents ermittelt und überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	RAID Logical Drives *<Name des Servers>* bei Adapter *<x> <Adaptername>*: *<logische Laufwerke>* RAID Level: *<Nummer> <RAID Level>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.14 RAID Logical Drives - Logische RAID-Laufwerke

Der Status der logischen RAID-Laufwerke von ServerView RAID wird über die ServerView Agents ermittelt und überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	RAID Logical Drives *<Name des Servers>* bei Adapter *<x> <Adaptername>*: *<logische Laufwerke>* RAID Level: *<RAID Level>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.1.15 RAID Physical Disks - Physische RAID-Laufwerke

Der Status der physischen RAID-Laufwerke von ServerView RAID wird über die ServerView Agents ermittelt und überwacht.

Symbol	Information	
	Display Name: *Server Name:* *Devices:* *Device Information:* *BMC Address:* *BMC DNS name:*	RAID Physical Disks *<Name des Servers>* bei Adapter *<x>* *<Adaptername>*: *<physische Laufwerke>* Größe: *<Kapazität>* *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.2 Status der Hardware-Subsysteme aktualisieren

Standardmäßig wird die Konfiguration der Hardware-Komponenten eines PRIMERGY Servers automatisch alle 4 Stunden ermittelt.

Versetzen Sie den Server vorübergehend in den Wartungsmodus. Nachdem der Wartungsmodus abgelaufen ist, ermittelt SCOM automatisch die Hardware-Komponenten neu. Ändern Sie alternativ das Zeitintervall der Ermittlung von Hardware-Komponenten, um ein Update zu erzwingen, indem Sie eine (vorübergehende) Außerkraftsetzung für die gesamte "Discovery Rule for Windows Server Health Collection" durchführen.

4.4.3 Ermittlung der benötigten Dienste

Die im Folgenden aufgeführten Dienste (Services) eines PRIMERGY Servers werden erkannt und überwacht.

4.4.3.1 ServerView Agents

Der Dienst "ServerView Server Control" ist der zentrale Dienst von Fujitsu zur Überwachung von PRIMERGY Hardware-Komponenten.

Monitor-Klasse: SCCI Management Software

Symbol	Information	
	Display Name: *Version:* *Server Name:* *Devices:* *BMC Address:* *BMC DNS name:*	ServerView Agent *<Version des Agenten>* *<Name des Servers>* Dienst "SrvCtrl.exe" *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.3.2 Windows Management Instrumentation (WMI)

Monitor-Klasse: WMI Management Software

Symbol	Information	
	Display Name: *Version:* *Server Name:* *Devices:* *BMC Address:* *BMC DNS name:*	Windows Management Instrumentation *<WMI-Version>* *<Name des Servers>* Keine *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.3.3 ServerView RAID

ServerView RAID verwaltet und überwacht alle RAID Controller von PRIMERGY Servern.

Monitor-Klasse: ServerView RAID

Symbol	Information	
	Display Name: *Version:* *Server Name:* *Devices:* *BMC Address:* *BMC DNS name:*	ServerView RAID *<Version>* *<Name des Servers>* Dienst "amService.exe" *<IPv4-Adresse des BMC>* *<FQDN des iRMC>*

4.4.4 Überwachung der Hardware-Komponenten

Die Überwachung der Hardware-Komponenten erfolgt mittels VB-Skript. Die Überwachungsskripts werden in regelmäßigen Abständen abgerufen (je nach Komponente alle 120 bis 180 Sekunden, frei einstellbar) und überprüfen den Status der Komponenten.

Alle Hardware-Komponenten werden in einer *Health Collection* gesammelt und im Integritäts-Explorer angezeigt (siehe Seite 31).

Wenn die Überwachungsfunktion für eine Komponente den Status *Kritisch* meldet, wird ein entsprechender Alarm erzeugt. Alarme bei *Warnungen* sind standardmäßig deaktiviert.

Wenn die Komponente wieder im Zustand OK ist, wird der Alarm aufgelöst und erscheint nicht mehr in der Ansicht *Active Alerts* (siehe Seite 29).

4.4.5 Überwachung der benötigten Dienste

Die erforderlichen Dienste werden von dienstspezifischen Monitoren überwacht. Der Gesundheitszustand der Dienste kann im Integritäts-Explorer sichtbar gemacht werden.

4.4.5.1 SCCI Management Software (ServerView Agents)

Der Zustand dieser Software-Komponente wird durch den folgenden Dienst ermittelt:

– ServerView Server Control (Service Name: *SvrCtrl.exe*)

Wenn die Überwachungsfunktion den Status *Kritisch* meldet, wird ein entsprechender Alarm erzeugt.

Wenn sich die ServerView Agents im Status *Critical* befinden, können die PRIMERGY Server nicht mehr überwacht werden.

Wenn die Komponente wieder im Zustand *OK* ist, wird der Alarm aufgelöst und erscheint nicht mehr in der Ansicht *Active Alerts* (siehe Seite 29).

4.4.5.2 Windows Management Instrumentation (WMI)

Der Zustand dieser Software-Komponente wird durch den Windows-Management-Instrumentation-Service (Service Name: *winmgmt*) ermittelt. Läuft dieser Dienst nicht, so wird der Zustand der WMI-Komponente auf *Kritisch* gesetzt.

Wenn die Überwachungsfunktion den Status *Kritisch* meldet, wird ein entsprechender Alarm erzeugt.

Wenn sich der WMI-Service im Status *Kritisch* befindet, können die PRIMERGY-Server nur eingeschränkt überwacht werden.

Wenn die Komponente wieder im Zustand *OK* ist, wird der Alarm aufgelöst und erscheint nicht mehr in der Ansicht *Active Alerts* (siehe Seite 29).

4.4.5.3 ServerView RAID Manager

Der Zustand dieser Software-Komponente wird durch den ServerView RAID Manager Service (Service Name: *amService*) ermittelt. Läuft dieser Service nicht, so wird der Zustand der ServerView RAID-Komponente auf *Kritisch* gesetzt.

Wenn die Überwachungsfunktion den Status *Kritisch* meldet, wird ein entsprechender Alarm erzeugt.

Wenn die Komponente wieder im Zustand *OK* ist, wird der Alarm aufgelöst und erscheint nicht mehr in der Ansicht *Active Alerts* (siehe Seite 29).

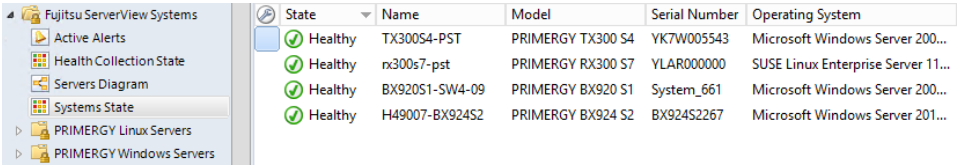
4.5 Ansichten

Der Integritätszustand in allen Ansichten wird durch die üblichen Symbole im Operations Manager dargestellt.

4.5.1 Vom MP *Fujitsu Systems Core Library* definierte Ansichten

Bei der Integration des Management Packs *Fujitsu ServerView Core Library* wird der Knoten *Fujitsu ServerView Systems* im Bereich *Überwachung* der SCOM-Konsole erstellt. In diesem Knoten werden die im Folgenden beschriebenen Ansichten angezeigt:

- Active Alerts
- Health Collection State
- Servers Diagram
- Systems State



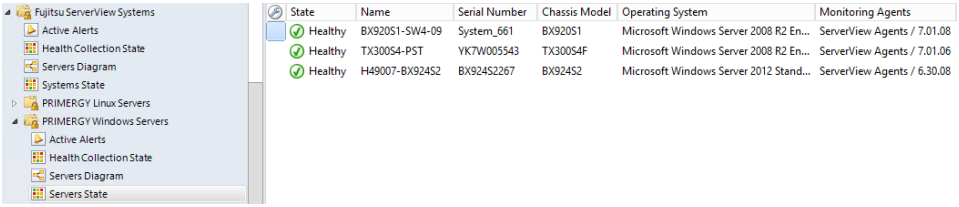
In diesen Ansichten werden alle Objekte angezeigt, die der Klasse zugewiesen sind, auf die die jeweilige Ansicht gerichtet ist. Welche Systeme in dieser Klasse enthalten sind, hängt davon ab, welche weiteren Fujitsu Management Packs installiert wurden, z. B. das Management Pack *Fujitsu PRIMERGY Windows Servers*.

Die vom Management Pack *Fujitsu ServerView Systems Core Library* installierten Ansichten enthalten alle Systeme, auf die sich Management Packs richten, die vom Management Pack *Fujitsu ServerView Systems Core Library* abhängen und eine einfache Übersicht über alle Fujitsu-Systeme bezwecken.

4.5.2 Vom MP *Fujitsu PRIMERGY Windows Servers* definierte Ansichten

Bei der Integration des Management Packs *Fujitsu PRIMERGY Windows Servers* wird der neue Knoten *PRIMERGY Windows Servers* unterhalb des Knotens *Fujitsu Systems* im Bereich *Überwachung* der SCOM-Konsole erstellt. In diesem Knoten werden die im Folgenden beschriebenen Ansichten angezeigt:

- Active Alerts
- Health Collection State
- Servers Diagram
- Systems State



Die vom Management Pack *Fujitsu PRIMERGY Windows Servers* installierten Ansichten richten sich nur auf PRIMERGY Windows Server und zeigen nur diese an.

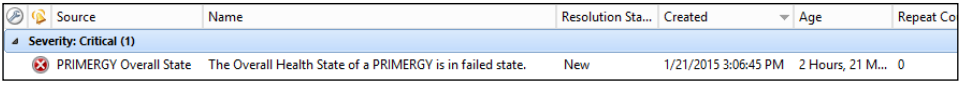
4.5.3 Ansicht "Active Alerts"

In den Ansichten *Active Alerts* werden alle Alarme angezeigt, die der Klasse zugewiesen sind, auf die die jeweilige Ansicht gerichtet ist. Nur Alarme mit dem Auflösungsstatus *Nicht geschlossen* werden angezeigt.

Folgende Ursachen können einen Alarm auslösen:

- Ist ein Komponenten-Monitor im Status *Kritisch*, wird für diese Komponente ein Alarm angezeigt.
  Dieser Alarm ist „selbstauflösend“, d. h. sobald die Ursache beseitigt ist, wird der Alarm aus der Ansicht wieder entfernt.
- Ein Ereignis (Event), für das eine Regel im Management Pack definiert ist, ist in die Windows Ereignisanzeige (Event Log) eines überwachten Servers eingetragen worden. Diese Alarme bleiben in der Anzeige stehen, bis sie explizit geschlossen werden.

Alarme werden standardmäßig nur durch Ereignisse erzeugt, die mit der Gewichtung *Kritisch* (Error) in die Windows Ereignisanzeige (Application, Operations Manager oder System) geschrieben worden sind. Ereignisse mit der Gewichtung *Warning* können auch angezeigt werden, wenn sie durch den Benutzer aktiviert werden.

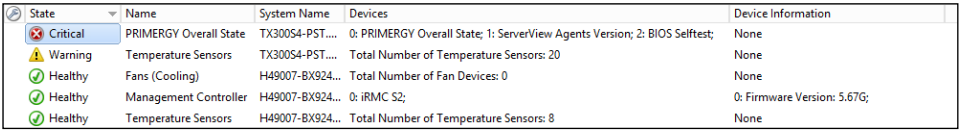


Alarme, die in den Auflösungsstatus *Geschlossen* versetzt werden, erscheinen nicht mehr in der Ansicht *Active Alerts*.

Für einige Alarme ist die Alarm-Unterdrückung aktiviert. In diesem Fall wird der Alarm nur einmal gemeldet. Alle weiteren Alarme dieses Typs werden lediglich im *Wiederholungszähler* gezählt. Um die Spalte mit dem *Wiederholungszähler* anzuzeigen, verwenden Sie die Einstellung zum Personalisieren der Ansicht.

4.5.4 Ansichten "Health State Collection"

Die Ansichten *Health State Collection* zeigen den Integritätsstatus der Hardware-Komponenten-Klasse an, auf die sich die jeweilige Ansicht richtet.



4.5.5 Ansichten "Diagram"

In den Ansichten *Diagram* wird die Infrastruktur der Fujitsu-Systeme grafisch dargestellt. Hier werden die Verbindung von Fujitsu-Systemen zu PRIMERGY Servern zu Modell-Gruppen und die Verbindung der Komponenten zu den PRIMERGY Servern dargestellt.

Wenn Systeme zu einer Gruppe gehören, wird neben dem Computersymbol ein ausgefüllter Kreis angezeigt. Diese Gruppe kann weiter aufgeklappt werden, um die vorhandenen Systeme sichtbar zu machen:

Des Weiteren wird der Zustand der Hardware- und Software-Komponenten eines Servers in der Ansicht *Servers Diagram* abgebildet. Dabei werden die Komponenten grafisch in Verbindung zu dem zugeordneten Server dargestellt.

Komponenten, die sich in einem gesunden Zustand befinden, werden in einer Fehlerfrei-Gruppe unterhalb des zugehörigen Servers zusammengefasst.

Sind mehrere Komponenten im Zustand *Warnung* oder Kritisch, so werden diese in entsprechenden Gruppen zusammengefasst und ebenfalls (parallel) unterhalb des PRIMERGY Servers dargestellt.

In der *Detailansicht* unter der Komponentenanzeige werden dann die ermittelten Instanzen einer Komponente und einige Eigenschaften angezeigt. Für jede Komponente werden folgende Eigenschaften angezeigt:

- *Display Name:* Name der Komponente
- *Server Name:* Name des Systems, zu dem die Komponente gehört
- *Devices:* Informationen über ermittelte Geräteinstanzen
- *Device Information:* zusätzliche Informationen über die Geräte, falls vorhanden
- *BMC Address:* IPv4-Adresse des integrated Remote Management Controllers
- *BMC DNS name:* FQDN (Fully Qualified Domain Name), falls vorhanden und wenn DNS auf dem iRMC aktiviert ist

4.5.6 Ansicht Server State

In den Ansichten *Server State* wird der Status aller Server angezeigt, die der Klasse zugewiesen sind, auf die die jeweilige Ansicht gerichtet ist.

State	Name	Serial Number	Chassis Model	Operating System	Monitoring Agents
Healthy	BX920S1-SW4-09	System_661	BX920S1	Microsoft Windows Server 2008 R2 En...	ServerView Agents / 7.01.08
Healthy	TX300S4-PST	YK7W005543	TX300S4F	Microsoft Windows Server 2008 R2 En...	ServerView Agents / 7.01.06
Healthy	H49007-BX924S2	BX924S2267	BX924S2	Microsoft Windows Server 2012 Stand...	ServerView Agents / 6.30.08

Die Eigenschaften des ausgewählten PRIMERGY-Servers werden in der Detailansicht unter dieser Ansicht angezeigt.

4.6 Integritäts-Explorer

Der Integritäts-Explorer kann aus den verschiedensten Ansichten gestartet werden. Er zeigt die Komponenten und Abhängigkeiten in einer Baumstruktur. Falls Komponenten im Zustand *Warnung* oder *Kritisch* sind, werden die entsprechenden Unterverzeichnisse in der Darstellung automatisch expandiert.

Im Integritäts-Explorer sind im rechten Fenster zwei unterschiedliche Darstellungen möglich: *Wissensdatenbankeintrag* und *Statusänderungsereignisse*. Unter der Registerkarte *Wissensdatenbankeintrag* werden Hinweise gegeben, was der Monitor anzeigt und welche Aktionen (Lösungen) möglich und zu empfehlen sind.

Unter der Registerkarte *Statusänderungsereignisse* werden alle Zustandsübergänge (*OK* <-> *Degraded* <-> *Error*) der ausgewählten Komponente aus dem linken Navigationsfenster angezeigt. Die Statusänderung wird nur für die erste Komponente angezeigt, die für die Statusänderung verantwortlich ist.

Im Falle eines Status ungleich *OK* wird die Komponente auf den Zustand *Degraded* oder *Error* gesetzt und die fehlerhafte Instanz im Integritäts-Explorer aufgeführt. Wenn für zwei oder mehrere Komponenten ein unterschiedlicher Integritätsstatus angezeigt wird, bestimmt die Instanz mit dem schwersten Fehler den Gesamtstatus der Gruppe.

<Komponente>_Components
: Instanzen der Komponente.

<Komponente>_HealthState

Degraded
: Mindestens eine Instanz der Komponente ist im Warnungszustand.

Error
: Mindestens eine Instanz der Komponente ist im kritischen Zustand.

<Komponente>_FailedComponent
: Ist eine Komponente im Zustand Degraded oder Error, so wird die fehlerhafte Instanz hier angezeigt.

4.7 Aufgaben für Fujitsu PRIMERGY Windows Server

Aufgaben sind Aktionen, die bei unterschiedlichen Ansichten eingeblendet und ausgeführt werden können. Aufgaben werden im Fenster *Aktionen* eingeblendet, wenn ein PRIMERGY Server markiert ist bzw. wenn PRIMERGY Hardware-Komponenten ausgewählt sind.

Aufgaben der PRIMERGY Server und Server-Komponenten

- Computer Management
- Remote Desktop
- Remote Desktop Console
- Delete PRIMERGY Server Component Inventory
- ServerView Raid Manager
- ServerView Remote Management iRMC

- ServerView System Monitor

4.7.1 Computer Management

Mit dieser Aufgabe wird die Microsoft Management Console (MMC-Anwendung) gestartet und der Zugriff auf die Daten des markierten PRIMERGY Servers ermöglicht.

4.7.2 Remote Desktop

Mit dieser Aufgabe wird der Remote Desktop gestartet, um sich auf dem PRIMERGY Server einzuloggen.

4.7.3 Remote Desktop Console

Mit dieser Aufgabe wird der Remote Desktop im Konsol-Modus gestartet, um sich auf dem PRIMERGY Server einzuloggen.

4.7.4 Delete PRIMERGY Server Component Inventory

Das Management Pack *Fujitsu PRIMERGY Windows Servers* verfolgt unter *HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-Win\PYServerData* die Anzahl der Komponenten, die für einen Server und die Registry des Servers ermittelt wurden.

Wenn einem Server neue Komponenten hinzugefügt werden, wird das Komponenten-Inventory erhöht und es wird ein informierender Alarm ausgelöst.

Wenn Komponenten fehlen, wird bei jeder neuen Ausführung des Skripts zur Komponentenermittlung ein Alarm ausgelöst (Standard: alle 4 Stunden).

Diese Aufgabe setzt die Inventory-Daten der Server-Komponenten zurück. Beim nächsten Komponentenermittlungszyklus werden neue Inventory-Daten erzeugt, ohne Alarme auszulösen.

Verwenden Sie diese Aufgabe, wenn Komponenten von einem Server entfernt wurden.

4.7.5 ServerView Raid Manager

Mit dieser Aufgabe wird die Web-Konsole des ServerView RAID Managers aufgerufen. Die Aufgabe wird für alle PRIMERGY Server angezeigt, und zwar selbst dann, wenn ServerView RAID Manager nicht auf dem Server installiert ist.

4.7.6 ServerView Remote Management iRMC

Diese Aufgabe wird verwendet, um die Konsole des iRMC (integrated Remote Management Controller) aufzurufen. Wenn ein DNS-Name für den iRMC gefunden wurde, wird der DNS-Name aufgerufen. Andernfalls wird die IPv4-Adresse des iRMC verwendet.

4.7.7 ServerView System Monitor

Diese Aufgabe wird zum Starten des Web-basierten ServerView System Monitors verwendet, mit dem PRIMERGY Server genau untersucht werden können.

Der Web-basierte System Monitor ist nur für PRIMERGY Server verfügbar, auf denen ServerView Agents ab V7.01 installiert sind.

Melden Sie sich bei PRIMERGY Servern mit älteren Versionen von SV-Agenten beim Server an (z. B. über die Aufgabe "Remote Desktop") und navigieren Sie über "Start – Alle Programme – Fujitsu – ServerView Suite – Agenten – System Monitor" zum System Monitor auf dem Server.

4.8 Ereignisse und Alarme

Dieser Abschnitt gilt nur für Alarme, für die Regeln in den Management Packs definiert sind.

Die Alarme bleiben so lange in der Ansicht *Active Alerts* sichtbar, bis sie explizit geschlossen werden (Zuweisung des Auflösungsstatus *Geschlossen*).

Alarme sind unabhängig von Monitoren und haben keinen Einfluss auf den Integritätsstatus des Servers. Sie dienen nur zur Anzeige eines Ereignisses.

Die folgenden Ereignisgruppen sind in das zentrale Management Pack integriert:

- HD.MIB
- NTCluster.MIB
- THRESHOLD.MIB
- Duplex Data Manager (DDM.MIB)
- QLogic Fibre Channel Adapter
- Emulex Fibre Channel Adapter (BE2NET, BE2ISCSI)
- Broadcom Network Adapter
- Intel Network Adapter (E1000, E100B, IE10G, ANS Miniport)
- Event Log Einträge der VB-Skripte im Management Pack

Für alle Alarme ist die Alarmunterdrückung aktiviert.

Die folgenden Alarme wurden in zusätzliche Management Packs für Kunden verschoben, die auch diese Alarme erhalten möchten, obwohl der Integritätsstatus des Komponentensubsystems vollständig von den Monitoren für den Subsystemintegritätsstatus (z. B. Temperaturen, RAID-Subsystem) abgedeckt ist.

- SC2.MIB
- ServerView-Raid

Eine Übersicht der integrierten Ereignisse ist in den Dateien *PRIMERGYServerEventsSCOM_e.pdf* und *windows_manual_elx.pdf* enthalten, die sich im Unterverzeichnis *Manuals* befinden.

Es sind nur Ereignisse integriert, die die Gewichtung *Warnung* oder *Kritisch* haben.

4.8.1 Aktivierung und Deaktivierung von Alarmen

Per Voreinstellung erzeugen alle Ereignisse mit der Gewichtung Kritisch einen Alarm und alle Ereignisse mit der Gewichtung *Warnung* erzeugen keinen Alarm.

Um die Standardeinstellungen zu ändern, überschreiben Sie diese im Bereich "Konfiguration" der SCOM-Konsole. Die Überschreibung muss danach in einem individuellen beschreibbaren Management Pack gespeichert werden.

4.9 Wissensdatenbank

Zu den Ereignissen und Alarmen ist eine Wissensdatenbank (Knowledge Base) vorhanden. Je nach Art des Alarms werden verschiedene mögliche Lösungen/Vorgehensweisen zur Fehlerbehebung angezeigt.

Diese Lösungen finden Sie auch in der Datei *PRIMERGYServerEventsSCOM_en.pdf* in der letzten Spalte der aufgeführten Ereignisse.

5. Anhang

5.1 Unterstützte PRIMERGY Server

Das ServerView Windows Server Integration Pack unterstützt PRIMERGY Server nicht direkt, sondern stützt sich auf ServerView Agents, die zur Bereitstellung von Server-Hardware-Daten auf dem Server installiert sind. Die PRIMERGY-Unterstützung hängt deshalb von den Agenten ab, die auf dem überwachten System installiert sind.

Die Release Notes der ServerView Agents enthalten detaillierte Informationen zur Unterstützung der PRIMERGY Server.

5.2 Einträge in der Ereignisanzeige des Operations Managers

Die VB-Skripte zum Erkennen und Überwachen der PRIMERGY Server und deren Komponenten schreiben im Fehlerfall Meldungen in die Ereignisanzeige des Operations Managers.

Diese Einträge sind auf den überwachten Servern unter dem Namen *Health Service Script* zu finden, während im Meldungstext angegeben ist, welches VB-Skript die Meldung erzeugt hat.

Über im MP definierte Regeln wird die Ereignisanzeige auf die oben erwähnten Einträge überprüft, und diese werden gegebenenfalls in der Ansicht *Active Alerts* angezeigt.

Einträge für Fehler sind eingeschaltet, Einträge für Warnungen sind ausgeschaltet. Für die Einträge der VB-Skripte sind in der Override-Datei Überschreibungen vorhanden.

5.3 Test-Einträge in der Windows Ereignisanzeige erzeugen

Um zu überprüfen, ob ein Alarm ein- oder ausgeschaltet ist bzw. ob er erkannt wird, können mit PowerShell Test-Einträge dieser Ereignisse (Events) in der Ereignisanzeige des betreffenden Servers angelegt werden.

5.4 Log-Dateien anlegen

Für die Fehleranalyse können Log-Dateien angelegt werden. Die Log-Dateien werden im *SVISCOM\SVISCOM-Win* Unterverzeichnis abgelegt, das in die System Environment-Variable *TEMP* eingetragen ist. In der Regel ist dies das Verzeichnis *C:\Windows\TEMP* (wobei bei diesem Beispiel *C:* für die Systempartition steht).

Logging-Optionen sind in der Datei SVSISCOMLog.ini in diesem Ordner definiert. Wenn die Datei nicht vorhanden ist oder von einer älteren Version des Management Packs erstellt wurde, wird eine Kopie der Datei mit dem Namen *SVISCOMLog.in_* für jede Serverermittlung im Ordner "%TEMP%\SVSCOM\SVISCOM-Win" erstellt.

Beachten Sie bitte, dass Änderungen an den Logging-Optionen nur der Datei *SVISCOMLog.in_* hinzugefügt werden. Die Datei *SVISCOMLog.ini* von einer älteren Version des ServerView Windows Server Integration Packs muss möglicherweise entsprechend aktualisiert werden.

*SVISCOMLog.in_* enthält Debug-Optionen für alle Ermittlungs- und Monitoring-Funktionen des Management Packs. Weitere Informationen siehe *SVISCOMLog.in_* auf einem beliebigen System.

Im Falle einer Fehleranalyse über die Log-Dateien gehen Sie bitte folgendermaßen vor.

- Benennen Sie die Datei *SVISCOMLog.in_* auf dem Zielserver in *SVISCOMLog.ini* um. Wenn bereits eine Datei mit dem Namen *SVISCOMLog.ini* vorhanden ist, überprüfen Sie, dass es alle Optionen der Datei *SVISCOMLog.in_ auch in der Datei SVISCOMLog.ini gibt.*
- Überprüfen Sie die Debug-Optionen (in der Datei "SVISCOMLog.in_" genau dokumentiert) für jede zu überwachende Funktion und setzen Sie sie auf den gewünschten Wert.

Es werden gegebenenfalls die folgenden Log-Dateien angelegt:

— *PRIMERGYServerDiscoveryTrace_<servername>.log*

— *PRIMERGYComponentsDiscoveryTrace_<servername>.log*

— *PRIMERGYComponentsMonitorTrace_<servername>_<component>.log*

— *PRIMERGYCommunicationMonitorTrace_<servername>_<component>.log*

— *PRIMERGYServerFCEvents_<servername>.log*

Diese Dateien sind für die weitere Analyse an den Fujitsu Support zu senden.

Wenn Sie die Erstellung von Log-Dateien wieder deaktivieren möchten, löschen Sie *SVISCOMLog.ini*, benennen Sie die Datei um oder ändern Sie die Logging-Optionen in der Datei.

5.4.1 Aktualität der Log-Dateien

Beim Import von Fujitsu Management Packs werden Log-Dateien nur dann umgehend erzeugt, wenn die Initialisierungsdatei bereits verfügbar ist.

Wenn das Management Pack bereits importiert wurde, werden je nach den in den Ermittlungs- oder Monitoring-Skripten festgelegten Ausführungsintervallen Log-Dateien erzeugt.

Schlimmstenfalls dauert es also 24 Stunden bis alle Log-Dateien erzeugt wurden.

Die Serverermittlung wird standardmäßig alle vier Stunden ausgeführt.

Die Komponentenermittlung wird standardmäßig alle 24 Stunden ausgeführt.

Wenn die Komponentenermittlung erfolgreich war, wird das Monitoring alle zwei bis drei Minuten ausgeführt.

Alternativ:

Um aktuelle Log-Dateien für die Ermittlung zu erstellen, bringen Sie den Server kurz in den Wartungsmodus und warten Sie, bis SCOM den Wartungsmodus beendet. Nach dem Ende des Wartungsmodus führt SCOM automatisch eine Server- und Komponentenermittlung durch.

5.5 Aktualisierung älterer Versionen des Windows Server Integration Packs

Das ServerView Windows Server Integration Pack unterstützt generell keine Updates. Es muss zunächst eine Deinstallation und dann eine neue Installation durchgeführt werden.

5.5.1 Migration von Versionen vor V8.0

Bei der Version V8.0 des ServerView Windows Server Integration Packs wurde der Weg für Management Packs für andere Betriebssysteme als Windows wie Linux geebnet. Um alle Fujitsu Management Packs in eine konsolidierte Struktur, sowohl in der SCOM-GUI als auch in der Management Pack-Suite, aufnehmen zu können, mussten die Klassen- und Objektnamen der alten Windows-MPs geändert werden.

Für Kunden, die eigene Management Packs für die Außerkraftsetzung oder sogar Skripte aus einer früheren Version verwenden, bedeutet dies leider ein wenig Arbeit. Anhang B enthält die alten und die neuen Klassen- und Objektnamen. Nehmen Sie den Anhang zu Hilfe, um alte Management Packs für die Außerkraftsetzung oder Skripte anzupassen.

Mit den folgenden Schritten sollten die meisten der erforderlichen Änderungen abgedeckt werden:

Gehen Sie bei allen (exportierten) Management Packs für die Außerkraftsetzung oder Skripten wie folgt vor:

- Ersetzen Sie "`Fujitsu.Servers.PRIMERGY.`" durch "`Fujitsu.Servers.PRIMERGY.Windows.`".
- Ersetzen Sie "`Fujitsu.Servers.PRIMERGY.Components.`" durch "`Fujitsu.Servers.PRIMERGY.Windows.`".
- Stellen Sie sicher, dass an keiner Stelle "`Fujitsu.Servers.PRIMERGY.Windows.Components.`" enthalten ist. Ersetzen Sie eventuelle Vorkommnisse durch "`Fujitsu.Servers.PRIMERGY.Windows.`".
- Fügen Sie bei MPs für die Außerkraftsetzung sowohl das MP *Fujitsu.ServerView.Library* als auch das MP *Fujitsu.Servers.PRIMERGY* als Referenz-MPs hinzu. Entnehmen Sie dem Anhang B die in diesen Management Packs definierten Klassen und fügen Sie diesen Klassen den Aliasnamen hinzu.

Mit diesen Schritten werden die meisten Klassen in individuellen MPs für die Außerkraftsetzung oder Skripten auf die neuen Namen migriert. Entnehmen Sie verbleibende Probleme den Meldungen, die SCOM oder PowerShell ausgeben.

5.6 Fehlersuche

5.6.1 ServerView System Monitor zur Untersuchung eines PRIMERGY Servers verwenden

Wenn bei einem PRIMERGY Server möglicherweise ein Problem besteht (z. B. bei einem schlechten Gesamtstatus von PRIMERGY) und die Problemursache nicht über SCOM ermittelt werden kann, kann der Server über den System Monitor genauer untersucht werden.

Markieren Sie den Server und verwenden Sie die Aufgabe "ServerView System Monitor", um den System Monitor zu starten.

Der Web-basierte System Monitor ist nur für PRIMERGY Server verfügbar, auf denen ServerView Agents ab V7.01 installiert sind.

Melden Sie sich bei PRIMERGY Servern mit älteren Versionen von SV-Agenten beim Server an (z. B. über die Aufgabe "Remote Desktop") und navigieren Sie über "Start – Alle Programme – Fujitsu – ServerView Suite – Agenten – System Monitor" zum System Monitor auf dem Server.

5.6.2 Kein Ereignis-Logging auf den Controller-Laufwerken

Nicht alle Controller-Laufwerke erzeugen automatisch Windows-Ereignis-Logs. Weitere Informationen zur Aktivierung des Ereignis-Logging finden Sie im Handbuch oder der Readme-Datei zu den jeweiligen Controller-Laufwerken.

5.6.3 Internet Explorer hat kein Java-Plugin

Die Installationsadresse von Internet Explorer ist in der System-Umgebungsvariablen „IEXPLORERPath“ gespeichert.

Wenn dieser Wert zu einem MSIE ohne Java-PlugIn führt, dann ändern Sie diese Umgebungsvariable in eine Adresse des IE mit installiertem Java-PlugIn.

5.6.4 Windows Installer-Logging aktivieren/deaktivieren (Debug)

Bei Problemen mit dem Installationsverfahren finden Sie weitere Informationen in diesem Artikel der Microsoft Knowledgebase (http://support.microsoft.com/kb/223300), in dem die Aktivierung und Deaktivierung des Logging beschrieben wird.

5.7 Tipps und bekannte Probleme

-

6. Anhang B

6.1 V8.0 Klassennamen und vorherige Namen

V8.0 Name	V8.0 Management Pack	Vorheriger Name
Fujitsu.ServerView.AllInstanceGroup	Fujitsu.ServerView.Library	-
Fujitsu.ServerView.Group	Fujitsu.ServerView.Library	Fujitsu.Servers.Group
Fujitsu.ServerView.ServersGroup	Fujitsu.ServerView.Library	Fujitsu.Servers.ServersGroup
Fujitsu.ServerView.System	Fujitsu.ServerView.Library	-
Fujitsu.ServerView.Server	Fujitsu.ServerView.Library	Fujitsu.Servers.Server
Fujitsu.ServerView.LogicalHardware	Fujitsu.ServerView.Library	Fujitsu.Servers.LogicalHardware
Fujitsu.ServerView.HealthCollection	Fujitsu.ServerView.Library	-
Fujitsu.ServerView.ManagementSoftware	Fujitsu.ServerView.Library	Fujitsu.Servers.ManagementSoftware

V8.0 Name	8.0 Management Pack	Vorheriger Name
Fujitsu.Servers.PRIMERGY.WindowsSeed	Fujitsu.Servers.PRIMERGY.WindowsSeed	-

V8.0 Klassennamen und vorherige Namen

V8.0 Name	8.0 Management Pack	Vorheriger Name
Fujitsu.Servers.PRIMERGY.Windows.ServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.ServersGroup
Fujitsu.Servers.PRIMERGY.Windows.BXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.BXServersGroup
Fujitsu.Servers.PRIMERGY.Windows.CXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.CXServersGroup
Fujitsu.Servers.PRIMERGY.Windows.MXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.MXServersGroup
Fujitsu.Servers.PRIMERGY.Windows.RXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.RXServersGroup
Fujitsu.Servers.PRIMERGY.Windows.SXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	-
Fujitsu.Servers.PRIMERGY.Windows.TXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.TXServersGroup
Fujitsu.Servers.PRIMERGY.Windows.XXServersGroup	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.XXServersGroup
Fujitsu.Servers.PRIMERGY.Windows.Server	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Server
Fujitsu.Servers.PRIMERGY.Windows.BXServer	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.BXServer
Fujitsu.Servers.PRIMERGY.Windows.CXServer	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.CXServer
Fujitsu.Servers.PRIMERGY.Windows.MXServer	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.MXServer
Fujitsu.Servers.PRIMERGY.Windows.RXServer	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.RXServer
Fujitsu.Servers.PRIMERGY.Windows.SXServer	Fujitsu.Servers.PRIMERGY.Windows	-
Fujitsu.Servers.PRIMERGY.Windows.TXServer	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.TXServer
Fujitsu.Servers.PRIMERGY.Windows.XXServer	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.XXServer
<entfernt>	-	Fujitsu.Servers.HealthCollection
Fujitsu.Servers.PRIMERGY.Windows.HealthCollection	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.HealthCollection

<entfernt>	-	Fujitsu.Servers.PRIMERGY.Processors
<entfernt>	-	Fujitsu.Servers.PRIMERGY.Memory
<entfernt>	-	Fujitsu.Servers.PRIMERGY.Fans
<entfernt>	-	Fujitsu.Servers.PRIMERGY.TemperatureSensors
<entfernt>	-	Fujitsu.Servers.PRIMERGY.Voltages
<entfernt>	-	Fujitsu.Servers.PRIMERGY.ServerNetworks
<entfernt>	-	Fujitsu.Servers.PRIMERGY.ServerStorage
<entfernt>	-	Fujitsu.Servers.PRIMERGY.ManagementController
<entfernt>	-	Fujitsu.Servers.PRIMERGY.PowerSupplies
<entfernt>	-	Fujitsu.Servers.PRIMERGY.PowerConsumption
<entfernt>	-	Fujitsu.Servers.PRIMERGY.RaidSubsystem
<entfernt>	-	Fujitsu.Servers.PRIMERGY.RaidLogicalDrive
<entfernt>	-	Fujitsu.Servers.PRIMERGY.RaidPhysicalDisk
<entfernt>	-	Fujitsu.Servers.PRIMERGY.PYOverallState
Fujitsu.Servers.PRIMERGY.Windows.Processors	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.Processors
Fujitsu.Servers.PRIMERGY.Windows.Memory	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.Memory
Fujitsu.Servers.PRIMERGY.Windows.Fans	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.Fans
Fujitsu.Servers.PRIMERGY.Windows.TemperatureSensors	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.TemperatureSensors

Fujitsu.Servers.PRIMERGY.Windows.VoltageSensors	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.Voltages
Fujitsu.Servers.PRIMERGY.Windows.ServerNetworks	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.ServerNetworks
Fujitsu.Servers.PRIMERGY.Windows.ServerStorage	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.ServerStorage
Fujitsu.Servers.PRIMERGY.Windows.ManagementController	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.ManagementController
Fujitsu.Servers.PRIMERGY.Windows.PowerSupplies	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.PowerSupplies
Fujitsu.Servers.PRIMERGY.Windows.PowerConsumption	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.PowerConsumptionPower
Fujitsu.Servers.PRIMERGY.Windows.RaidSubsystem	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.RaidSubsystem
Fujitsu.Servers.PRIMERGY.Windows.RaidLogicalDrives	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.RaidLogicalDrive
Fujitsu.Servers.PRIMERGY.Windows.RaidPhysicalDisks	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.RaidPhysicalDisk
Fujitsu.Servers.PRIMERGY.Windows.PYOverallState	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.Components.PYOverallState
Fujitsu.Servers.PRIMERGY.Windows.ManagementClientSoftware	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.ManagementClientSoftware
Fujitsu.Servers.PRIMERGY.Windows.WMIManagemen	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.WMIManagement
Fujitsu.Servers.PRIMERGY.Windows.RaidManagement	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.RaidManagement
Fujitsu.Servers.PRIMERGY.Windows.SCCIManagement	Fujitsu.Servers.PRIMERGY.Windows	Fujitsu.Servers.PRIMERGY.SCCIManagement